REMARKS

[0002] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1, 9, 12, 15, 17, 19 and 21-24 are currently pending.
- Claims 1 and 17 are amended herein.

Support for Claim Amendments

[0003] Claims 1 and 17 were amended for reasons of clarity, and do not recite additional elements for which an indication of support is required.

Cited Documents

[0004] The following documents have been applied to reject one or more claims of the Application:

- **Hamann**: Hamann et al., U.S. Patent Application Publication No. 2002/0026578
- **Dancs**: Dancs, U.S. Patent No. 6,108,789
- **Skomra**: Skomra, U.S. Patent Application Publication No. 2005/0076198

Claims 1, 9, 12, 15, 17, 19 and 21-24 Are Non-Obvious

[0005] Claims 1, 9, 12, 15, 17, 19 and 21-24 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Hamann in view of Dancs and Skomra. In response, the Applicant respectfully traverses the rejection.

Independent Claims 1, 9, 17, 21 and 23

[0006] The Applicant submits that the Office has not made a *prima facie* showing that independent claims 1, 9, 17, 21 and 23 are obvious in view of the combination of

Hamann, Dancs and/or Skomra. The Applicant submits that Hamann, Dancs and/or Skomra do not teach or suggest at least the following features of these claims (with emphasis added to identify aspects for discussion):

> **1. (Currently Amended)** A method comprising:
> determining if a smartcard is operatively available, said smartcard having smartcard memory;
> requiring entry of a password and authentication by the smartcard;
> identifying at least one root certificate stored in said smartcard memory;
> reading said at least one root certificate from said smartcard memory;
> storing said at least one root certificate in a computing device having computer memory operatively coupled to said smartcard, wherein the storing comprises copying said at least one root certificate from the smartcard to a certificate store maintained in said computer memory;
> determining when said smartcard is no longer operatively available to the computing device; and
> **erasing said root certificate from said computing device when said smartcard is no longer operatively available.**

[0007] Claim 1 recites in part, "erasing said root certificate from said computing device when said smartcard is no longer operatively available." The Office cites Skomra as teaching this element (Office Action mailed 11/13/2009, page 4). The Applicant respectfully submits that Skomra's disclosure fails to teach or suggest the recited claim language.

[0008] The Skomra reference teaches an authentication system (e.g., see Skomra at Title) providing a digital certificate authenticating the identity of a user at an endpoint device over a network (e.g., see Skomra at the Abstract). Referring to Skomra at Figure 1, the secure storage 35 includes the user's certificate 19. At paragraph [0042], Skomra describes how the digital certificate certifies the user's endpoint device 23 as an authorized device 24. This condition is reversed when the smart card 35 is removed,

turning the endpoint device 23 into an unauthorized endpoint device 25 (see Skomra at paragraphs [0113] and [0114], and particularly the last sentence of [0114]. Accordingly, removal of the smart card separates the smart card secure storage 35 from the device 23, thereby removing its authorization.

[0009] However, removal of the smart card, to turn the endpoint device into an unauthorized device, does not anticipate, teach or suggest "erasing said root certificate from said computing device when said smartcard is no longer operatively available," as recited. In fact, Skomra does not teach erasing any certificate, because Skomra instead teaches removing the smart card. Thus, Skomra teaches removal of a smart card as a different technical solution to un-authorizing a device, and does not teach or suggest erasure of a certificate.

[0010] The Office (at page 4 of the Action mailed 11/13/2009) points to Skomra at paragraph [0114], and suggests that Skomra teaches "erasing said root certificate from said computing device when said smartcard is no longer operatively available." For at least the reasons noted below, the Applicant respectfully submits that Skomra's disclosure fails to teach or suggest the recited claim language.

[0011] At paragraph [0114], Skomra teaches provision for "authenticating a user and enabling an authorized user endpoint device to access proprietary services." Moreover, Skomra teaches that the authentication of an endpoint device is dependent on the association with the authenticated user, and that the authentication of the endpoint device should end, if the association with the authenticated user ends. Skomra teaches that the removal of a smart card device 35 deprives the endpoint device 23 of the certificate 19, which converts the device 23 from an authorized device 24 to an unauthorized device 25.

[0012] Thus, at paragraph [0114], Skomra fails to teach or suggest "erasing said root certificate." Instead of an erasure, Skomra teaches removal of a smart card. While both Skomra's teaching, and the recitation by claim 1, result in a similar circumstance, i.e., decertification of a computing device in accordance with loss of a root certificate, there are significant differences in the method by which Skomra and the elements of claim 1 operate, and significant differences in the benefits of the two methods.

[0013] The Applicant's method, as recited by claim 1, is not taught or suggested by the cited documents of record, and additionally provides significant advantages not available to the cited documents of record. In particular, in one embodiment or version, the Applicant's method is configured to "allow any other applicable logic in computer 130 [to] access or otherwise use root certificate 214 as needed to perform certificate supported processes" (see the Applicant's paragraph [0063]). **Thus, for example, the method of claim 1, as taught by the Applicant's specification, may allow *existing applications* to look to the location, i.e., the Certificate Store, to which they are programmed to look for a Root Certificate**. This is in contrast to the cited documents discussions by Skomra, which indicate that applications requiring a Root Certificate must look to the smart card attached to the user device.

[0014] This distinction is profound, in that the method of claim 1 allows **existing software**, such as browsers, **to operate without modification**, and to find Root Certificates in the expected location, i.e., the Certificate Store. In contrast, the teachings of Skomra would require that applications—such as browsers seeking to authenticate, or a word processor seeking to open a remote file—to be modified to read certificates **from an alternate location associated with the smart card**. Such

requirements for modification would render existing software ineffective, and production of replacement software would result in prohibitive cost.

[0015] Skomra is representative of the cited documents, in that it fails to teach or suggest reading the root and/or user's certificate, and writing it. In fact, in contrast to the recitation of claim 1, **reading a certificate from the smart card is typically not possible**. Referring to the Hamann reference at the end of paragraph [0005], Hamann teaches that "Modern smart cards are able to perform the signing operation inside the card. At the same time, they do not provide any functionality to export the private key to the outside." Thus, the cited documents generally provide no mechanism to read certificates from a smart card, and therefore to write such certificates to computer memory and to later erase them.

[0016] Thus, the Applicant respectfully submits that Skoma does not support "erasing said root certificate", as recited. Moreover, even in combination, Hamann, Dancs and/or Skomra fail to teach or suggest all of the elements and features of this claim. Accordingly, the Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claims 9, 17, 21 and 23

[0017] Claims 9, 17, 21 and 23 were rejected in a rejection (see Office Action mailed 11/13/2009, pages 3 and 4) that was unified with the rejection of claim 1. These claims are allowable for reasons similar to the reasons that claim 1 is allowable over the documents of record, and the remarks from above are incorporated herein by reference. These claims may also be allowable for the additional features that each recites.

Dependent Claims 12, 19, 22 and 24

[0018] Claims 12, 19, 22 and 24 ultimately depend from independent claims 9, 17, 21 and 23, respectively. As discussed above, claims 9, 17, 21 and 23 are allowable over the cited documents. Therefore, claims 12, 19, 22 and 24 are also allowable over the cited documents of record for at least their dependency from an allowable base claim. These claims may also be allowable for the additional features that each recites.

Conclusion

[0019] For at least the foregoing reasons, all pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that would prevent allowance of this application, **the Applicant requests that the Examiner contact the undersigned representative before issuing a subsequent Action.**

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/David S. Thompson 37954/ Dated: 16 Feb 2010

David S. Thompson
Registration No. 37954
509-944-4735
davidt@leehayes.com

David A. Divine
Registration No. 51275
509-944-4733
daved@leehayes.com